Analytical evaluation of RSA and AES using Windows Azure for cloud computing environment

Ayman Bassam Nassuora,[a] Syed Asfandyar Gilani[a], Muhammad Inaam ul Haq[b]

[a] Department of Management Information Systems, City University College of Ajman (UAE)
a.bassam@cuca.ae

[b] Department of Computer Science, COMSATS University, Pakistan

Abstract Cryptography is a very useful tool to protect the properties of data like integrity, privacy, confidentiality in any environment. This paper explores some useful aspects of cryptography in cloud computing environment. There are different types of encryption algorithms used in order to ensure the data security. These algorithms are of different types like symmetric, a symmetric and hashing algorithms. The objective of this paper is performance analysis of selected set of algorithms on the basis of different parameters, so that the best out of all these options is chosen or combinations of some of them can be utilized to secure data in cloud computing environment. The algorithms included in this study are RSA, AES. The parameters which are used for performance analysis are CPU utilization, running time of the code, data encryption capacity. These are the performance parameters which are calculated for every algorithm in cloud based environment i.e. windows azure simulator by utilizing visual studio IDE and profiler services by integrating windows azure SDK. The interpretation of these results are done by using various graphs which shows trend of a particular algorithms on basis of time of encryption and decryption.

Keywords: cryptography, cloud security, RSA, AES, Windows Azure.

1 INTRODUCTION

Cloud computing is very complex in nature. It uses different techniques which are not visible on front end. Virtualization technology is used to achieve high performance computing in cloud computing concept. Virtualization is used for the optimize utilization of resources to gain performance. In this technique multiple VMs called virtual machines are set up on single server performing different tasks. In this way less number of servers is used but ratio of tasks to be performed is increased on single server. This technique has lot of advantages for cloud provider e.g.; he can save cost that can be used for buying more servers and has to be spent on maintenance of existing servers. So cost is saved and optimum resource utilization is also achieved [1].

Data security i.e. data privacy, data integrity and confidentiality are the main concern of any small or large organization before moving to cloud technologies. The owner of any firm when think of shifting towards cloud trend he has lot of questions in mind but security of its data is the first and most important concern. This is basically a big hurdle in shifting towards cloud. When a company using cloud all its data is stored on cloud servers.[2] The data is travelling via internet the first risk is started from this node as data packet are being provider. In the 3rd scenario cloud provider only provide the computing resources generally called hardware rest of layers end user get from another party.

So the organization providing SAAS to End user pay to cloud provider for infrastructure i.e. for hardware usage and End User pay to SAAS provider for services. In cloud computing

there are four deployment model i) private cloud ii) community cloud iii) public cloud iv) Hybrid Cloud. In private cloud scenario, single organization like multinational having the power to bear all cost maintains its own cloud called private cloud it is most restricted and secure mechanism e.g. the data center of an organization. Small or medium size organizations cannot afford this type of cloud sent from the company network to cloud the data packet has to take different routes to go to the destination servers on cloud. During this path any intruder can temper this data if he is successful then data become useless for the organization [3].

2 LITERATURE REVIEW

In cloud computing there are three delivery models i)Software as Service (SAAS) ii) Platform as a Service(PAAS) iii) Infrastructure as a Service(IAAS).In SAAS: in this case cloud provider manage all setup like software middle ware i.e. platform and infrastructure in other words complete running application[4]. End User of the system pays to the cloud provider for usage of the system on basis of time i.e. number of hours he utilized the cloud services. The responsibility to provide the services, cloud maintenance and security of data and other things is on cloud provider and he is bound according to different acts like SOX, HIPAA etc. In second scenario as mention PAAS, cloud provider provides the middle ware (plat farm as service) e.g. common runtime environment, End User of the system has to pay to the person or Organization providing the user SAAS and for middle ware he pays to cloud.

Group of organization having common goals like banks, cooperate organizations, enterprise business units combine together to form a community. The cloud used by the same interest group is called community cloud. Public cloud is the cloud setup which is formed for public usage for the common people from security point of view this is least secure cloud environment. Hybrid cloud are developed according to custom requirement of people or organization in which two cloud deployment strategies are merged together to form a hybrid philosophy [5]. Cloud provider has lot of servers when data sent from client end to cloud server a lot of data mining activity is done to store the data because cloud provider has data of so many organizations to store on specific space on the server. In this activity it is possible that the integrity of the data compromised. So there is risk of losing the data integrity. The data of any organization like banks or any other multinationals is highly confidential. It contains customer information like their bank account details in case of banks data. Every organization has some type of data which is highly confidential on which base of business strongly depends. If due any reason confidently of data is compromised it is harmful for business.

The suggestions for using different security algorithms are given in [6] to resolve security concern of cloud computing environment The problem faced by cloud provider discussed in [7]and solution to overcome those problems is also given. Windows Azure is used as a platform as a service to develop applications that can be deployed in Microsoft cloud computing environment, data centers. It is very feature rich environment for developing enterprise level applications. Windows Azure provides cloud computing emulator to debug, run, test and check the performance of the code which ultimately runs in the cloud computing environment

3 SIMULATION TECHNIQUES

Visual studio 2010 and windows azure SDK is used to design the application to test the different parameters of RSA and AES for comparison. The screen given below shows a browse button at start, user can browse files of different sizes and select algorithm from dropdown list and press execute button to run the process. An option is given below to specify number of key bits.

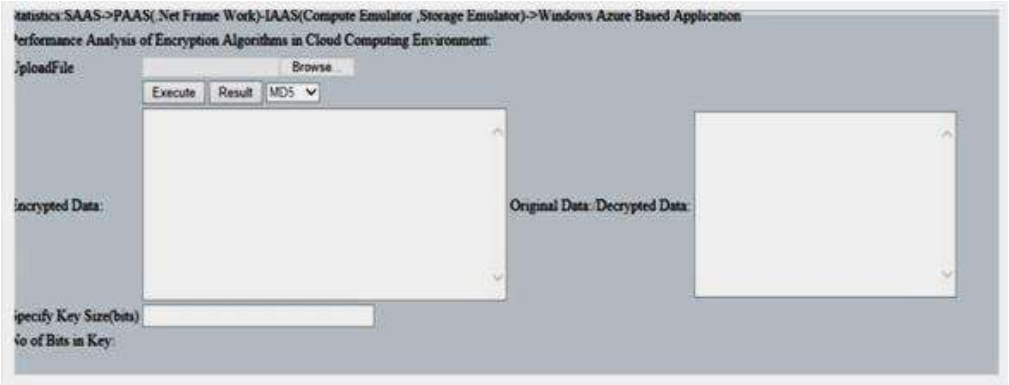

Figure 1: RSA and AES Windows Azure Simulation

4 SIMULATION TECHNIQUES

The table of values is taken by running the application developed on cloud environment. It shows the different readings of encryption and decryption time against different key size (bits) for RSA.

Table 1: RSA Encryption and Decryption Time

Key Size in bits	Encryption Time(ms)	File size	Decryption Time(ms)
512	10	30 bytes	12
768	11	30 bytes	13
1024	210	30 bytes	215
1280	220	30 bytes	225
1536	275	30 bytes	285
1792	293	30 bytes	308
2048	690	30 bytes	711
2304	750	30 bytes	800
2560	830	30 bytes	860
2816	1020	30 bytes	1040
3072	1199	30 bytes	1306

3328	1611	30 bytes	1699
3584	1887	30 bytes	2019
3840	3055	30 bytes	3070
4096	3684	30 bytes	3284

The graph is plotted between key size and decryption time of RSA. It shows that if key size is increased the time to decrypt the data is also increased. It means that by increasing key size more computation power and resources are required.

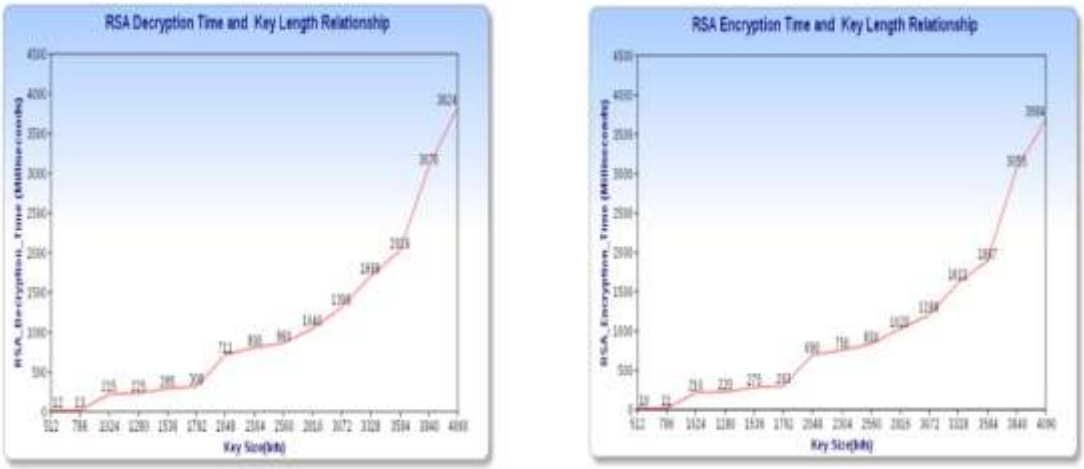

Figure 2: Graph between RSA Decryption Time and Key

The graph is plotted between key size and encryption time of RSA. It shows that if key size is increased, the time to encrypt the data is also increased. But in case of decryption, the time value is much greater as compared to encryption.

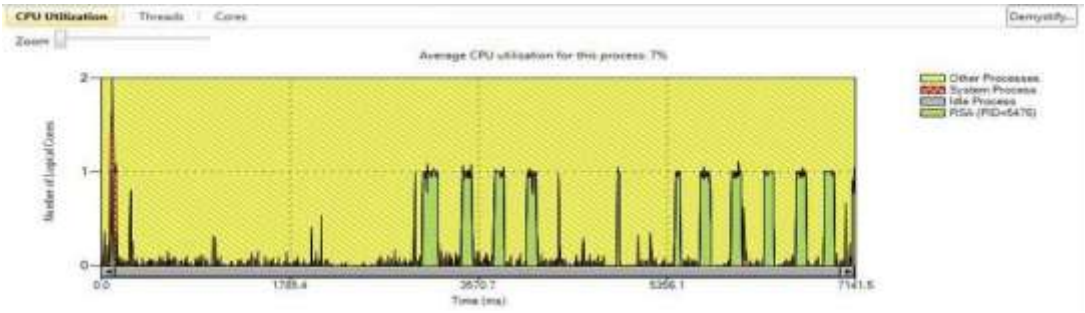

Figure 3: RSA CPU Utilization

There are three types of AES version are available these are AES-128, AES-192 and AES-256. But the focus of this study is AES-256.The block size in any version of AES is fixed and it is of 128 bits. The table given below gives the statistics about the AES-256 version in cloud simulator (cloud computing environment).

AES-256 Encryption Time (ms)(Average)	File size	AES-256 Decryption Time (ms)(Average)
6	200KB	7
11	400KB	13
20	600KB	30
29	800KB	34
74	1MB	85
83	2MB	97
129	3MB	183

Figure 4: AES CPU Utilization

The graph given below gives the relationship between file size of input data and corresponding values of Encryption time taken by AES-256.The graph shows that as the size of input file increases the corresponding encryption time also increases but not in linear fashion. The AES encryption time is much higher for large data input files as compared to small data KB files. The trend rapidly increased if we feed large size file as input to this algorithm.

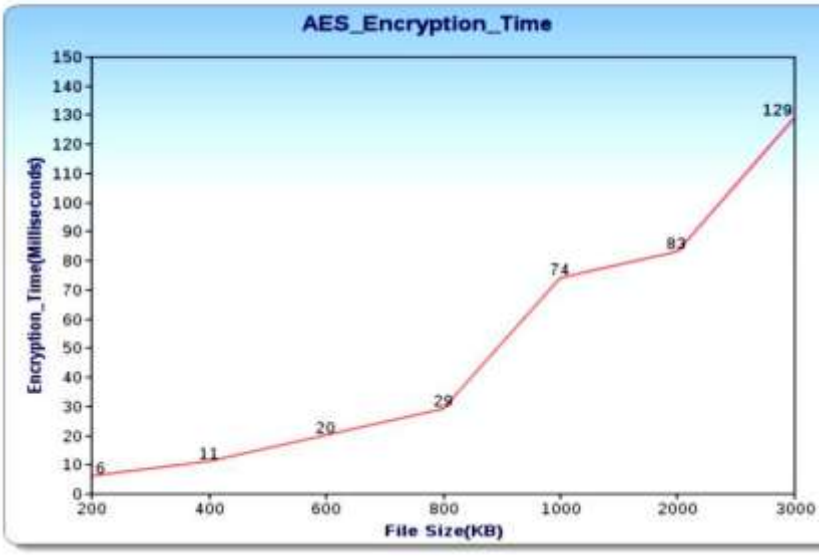

Figure 5: Graph between AES Encryption Time and File size

The graph given below gives the relationship between file size of input data and corresponding values of decryption time taken by AES-256.The graph shows that as the size of input file increases the corresponding decryption time also increases but not in linear fashion .The AES decryption time is higher as compared to encryption time. For large data input files it is more as compared to small data KB files. The trend rapidly increased if we feed large size file as input to this algorithm.

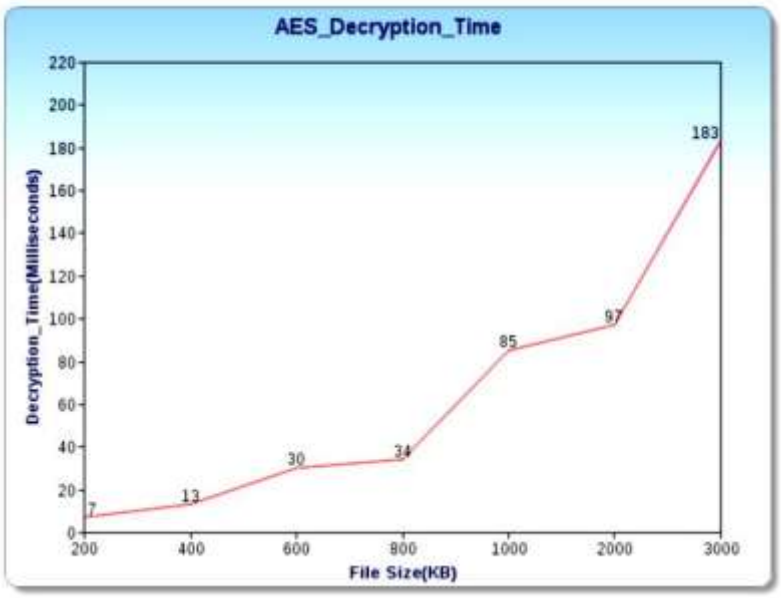

Figure 6: Graph between AES Decryption Time and File size

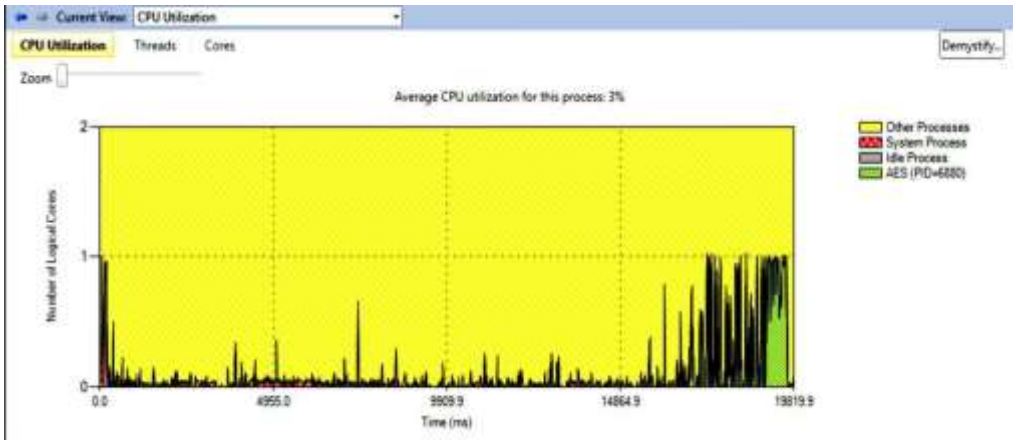

Figure 7: AES CPU Utilization

5 CONCLUSION

There are different types of algorithm which are available for providing data security. In this paper AES, which is symmetric and RSA asymmetric are selected to find the best one to provide data security in cloud computing environment. The performance of all these algorithms analyzed by using different parameters like data encryption capacity, strength on

basis of key, data encryption and decryption time. The environment used for this purpose is windows azure. It provides PAAS and IAAS. The analysis process after comparing all these parameters that are analyzed through simulator developed using windows azure SDK concludes that AES is best option because it is fast and its data encryption capacity is high. RSA is most secure but it require much resources and computation power its data encryption capacity is much low as compared to AES.

6 FUTURE WORK

In future a complete system i.e. security model for cloud computing environment can be developed which cover following features:

i. All possible encryption algorithms which best suitable for cloud computing environment are implemented in the system.
ii. The encryption and decryption option for every suitable user can be given before sending its data to cloud.
iii. A feature in which user can able to encrypt data with key with one algorithm and then able encrypt key by some different algorithm is provided.
iv. Authentication mechanism can be adopted so that only valid user able accesses the system for encryption and decryption of data.

References

[1]Dong Xu, "Cloud Computing: an Emerging Technology", International Conference On Computer Design And Applications (ICCDA 2010), Volume-1, Pgs (100-104).

[2] Pearson, S., Benameur, A., Privacy, Security and Trust Issues Arises from Cloud Computing, Cloud Computing Technology and Science (CloudCom), IEEE Second International Conference 2010, On page(s): 693-702.

[3]Iankoulova, I.; Daneya, M., Cloud computing security requirements: A systematic review, Research Challenges in Information Science (RCIS), Sixth International Conference on, 2012, On page(s): 1 - 7.

[4]. Radhika G, Satyanarayana K. V, Tejaswi A (2013)."Efficient Framework for Deploying Information in Cloud Virtual Datacenters with Cryptography Algorithms". International journal of computer trends and technology. [5] Sujay. R , "Hybrid Cloud:A New Era" , International Journal of Computer Science and Technology Vol. 2, Issue 2, June 2011.

[6]. Kaur M, Mahajan M. (2013). "Using encryption Algorithms to enhance the Data Security in Cloud". International journal of communication and computer technologies.

[7]. Arora R, Parashar A (2013). "Secure User Data in Cloud Computing Using Encryption".

[8]. Padhy R, P Patra, M. R., &Satapathy, S. C. (2012). "WINDOWS AZURE PAAS CLOUD: AN Overview". International Journal of Computer Application.

[9]. Zotos K., Litke A. "Cryptography and Encryption"

[10]. Subashini S, Kavitha V. (2011). "A survey on security issues in service delivery models of cloud computing". Journal of Network and Computer Applications

[11]. Jose N, A C K (2013)."Data Security Model Enhancement in Cloud Environment". IOSR Journal of Computer Engineering(IOSR-JCE)

[12]. Wei Lu, Jared Jackson, and Roger Barga, "AzureBlast: A Case Study of Developing Science Applications on the Cloud", Proceedings of the 1st Workshop on Scientific
Cloud Computing (Science Cloud 2010), Association for Computing Machinery, Inc., 21 June 2010

[13] A. Velte, T. Velte, and R. Elsenpeter, Cloudcomputing: a practical approach, New York:McGraw-Hill, 2010.

[14] Madhurima, Vandana, Madhulika "Windows Azure Platform: an Era for Cloud Computing", International Journal of Computer Science and Information Technologies, Vol. 2 (2), 2011, 621-623. Amit Chauhan, et.al. Int. J. EnCoTe, v01012011, 11-17 Available

[15] Rimal, B., Choi, E., and Lumb, I. (2009). A Taxonomy and Survey of Cloud Computing Systems. In Fifth International Joint Conference on INC, IMS and IDC, pages 44–51. IEEE.

[16] N. Saravanan, A. Mahendiran, N. Venkata Subramanian and
N. Sairam "An Implementation of RSA Algorithm in Google Cloud using Cloud SQL" Research Journal of Applied Sciences, Engineering and Technology 4(19): 3574-3579,2012.

[17]H. Jin, S. Ibrahim, T. Bell, L. Qi, H. Cao, S. Wu, and X. Shi, "Tools and technologies for building clouds", in Cloud Computing:Principles, Systems and Applications, N. Antonopoulos and L.Gillam, Eds, London:Springer, 2010. [18]Lizhe Wang, Gregor von

[19] Sang Ho. Na, Jun-Young Park, Eui- Nam Huh, Personal Cloud Computing Security Framework, Service Computing Conference (APSSC), Dec 2010 IEEE, On page(s): 671-675.

[20]Cloud Security Alliance Guidance,"Security Guidance For Critical Areas of Focus In Cloud Computing Vl.0",www.cloudsecurityalliance.orglguidance/csaguide.v1 .0.pdf, published April 2009.

[21] Farzad Sabahi," Cloud Computing Security Threats and Responses," 2011

[22]Dai Yuefa, Wu Bo, Gu Yaqiang, Zhang Quan and Tang Chaojing, "Data Security Model for Cloud Computing," Proceedings of the 2009 International Workshop on Information Security and Application (IWISA 2009) Qingdao, China, November 21-22, 2009.

[23]Deyan Chen and Hong Zhao, "Data Security and Privacy Protection Issues in Cloud Computing," International Conference on Computer Science and Electronics Engineering, 2012.

[24] Reynolds, E. and Bess, C. (2009). Clearing Up the Cloud: Adoption Strategies for Cloud Computing. Cutter IT Journal, 22(6/7):14–20.

[25] Rimal, B., Choi, E., and Lumb, I. (2009). A Taxonomy and Survey of Cloud Computing Systems. In Fifth International Joint Conference on INC, IMS and IDC, pages 44–51. IEEE.

[26] Rajkumar Buyya, Chee Shin Yeo, Srikumar Venugopal, James Broberg , Ivona Brandic "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing " Journal of Elsevier- Future Generation Computer Systems (2009).

[27] N. Saravanan, A. Mahendiran, N. Venkata Subramanian and N. Sairam "An Implementationof RSA Algorithm in Google Cloud using Cloud SQL" Research Journal of Applied Sciences, Engineering and Technology 4(19): 3574-3579, 2012.

[28] Buyya, Venugo, "Cloud Computing and emerging IT platforms: Vision, hype, and reality for delivering Computing as the 5th Utility", [2008].

[29] Keahey, Fortes, Freeman, "Science Clouds:Early Experiences in Cloud Computing for scientific applications" [2008].

[30] Rohit Bhadauria and Sugata Sanyal, A Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques. International Journal of Computer Applications, Volume 47- Number 18, June 2012, On page(s): 47-66.
[31] Puneet Jai Kaur, Sakshi Kaushal, Security Concerns in Cloud Computing, Communication in Computer and Information Science Volume 169 in 2011, On page(s): 103-112.
[32] Shui Zhang, Shufen Zhang, Xuebin Chen, Xiuzhen Huo, Cloud Computing Research and Development Trend, Second International Conference on Future Networks (ICFN), IEEE Publications, January 2010, On page(s): 93-97.
[33] Cloud Security Alliance "Top Threats to Cloud Computing V1.0", March 2010.
[34] Reynolds, E. and Bess, C. (2009). Clearing Up the Cloud: Adoption Strategies for Cloud Computing. Cutter IT Journal, 22(6/7)

Dr. Ayman Bassam Nassuora has a Ph.D. in Information Systems from University Utara Malaysia. He is currently serving as Associate Professor and Head of the MIS department at City University College Ajman. He has over 18 years of teaching & research experience at various universities around the world. His specific area of expertise is Knowledge Management and Database Systems.